Northway
Solutions Group

BYOD: Developing a Testing Strategy That Works

October 01, 2012 | Brian Copeland

The movement of corporate entities toward Bring Your Own Device (BYOD) is in full swing. Companies in reaction to financial pressures are looking at all options for reducing costs, including a reduction in the number of corporate owned and supported mobile devices. Gone are the days that virtually every member of the IT staff has a corporate sponsored smart phone. Corporations have embraced the BYOD trend as a means to manage skyrocketing operational costs.

Most employees don't understand what BYOD means to them. You are basically turning your personal device over to the company to manage as their asset. You sign over you right to decide what you put on your device (e.g. Angry Birds), and you subject your device to the will of the company. In many cases you sign away your right to you own personal data, and in case of termination or non-compliance may have your device wiped of all data including your personal email, texts, application data, and potentially even your personal photos. The company must take these seemingly harsh steps to protect themselves and the potential sensitive data that you may have accessed through the corporate network.

Read any blog or article about BYOD and you will quickly conclude that security is the number one concern of companies as they move toward the strategy. The core focus of solutions that manage the delivery of corporate solutions to mobile devices is the ability to provide adequate security for the company. These Mobile Device Management (MDM) solutions have robust policies, security and workflow that ensure that the employee doesn't do anything to their device that puts the company in jeopardy. Security is an extremely important part of reducing the risk to the organization and needs to be vigorously tested as part of an overall testing strategy; however, security testing should not be the only focus of the testing team.

I had the opportunity to meet with and interview a senior level the QA leader at a major financial institution headquartered in the Midwest about their BYOD testing initiative. This QA team is responsible for the testing of the corporate BYOD implementation. Below are the answers to the questions we discussed. The answers highlight the challenges that BYOD initiatives present to the testing organization and the development of a robust testing strategy for BYOD.

Q: *What is your greatest concern as you consider how to test your organization's BYOD implementation?*

A: "Security absolutely! It's all about security. Functionality takes a distant second. Functionality is being assessed primarily through user acceptance testing. We really don't have a solid set of requirements so determining what to test is difficult. The first application to be delivered is email with very basic read and send."

Q: *What are the primary components of your strategy to test the BYOD initiative?*

A: "We don't have a good strategy. This is largely due to the lack of a dedicated budget for this initiative. This is a brand new technology for the team. The challenge is exponential with BYOD as there are so many combinations of device, OS and carrier."

Q: *Have you discovered any changes you needed to make to the way you approach testing with BYOD?*

A: "Absolutely. This is a whole new world of testing. While a lot of what we traditionally do for internal application testing remains consistent, there is now this whole new technology. It used to be that there was one supported corporate computer and browser standard across the bank, but with BYOD that is thrown completely out the window."

Q: *How have you used technology to support testing of your BYOD implementation?*

A: "We are still trying to figure it out. Our first efforts were very manual and limited, with just a few devices to test on."

Q: *What has been your device testing strategy for BYOD?*

A: "We had a Blackberry and rented an iPhone, and then found a few people who had devices. We have had to assume that the development team is competent and knows what they are doing. We are finding out that they were just as constrained as we were. We are limiting risk by just deploying email as a first step."

Q: *What recommendations would you make to an organization that is just starting down the BYOD road?*

A: "I wished we had recognized earlier that the BYOD initiative was coming so we could research testing strategies and techniques. By the time we figured it out it was too late to become educated. We had to just do our best."

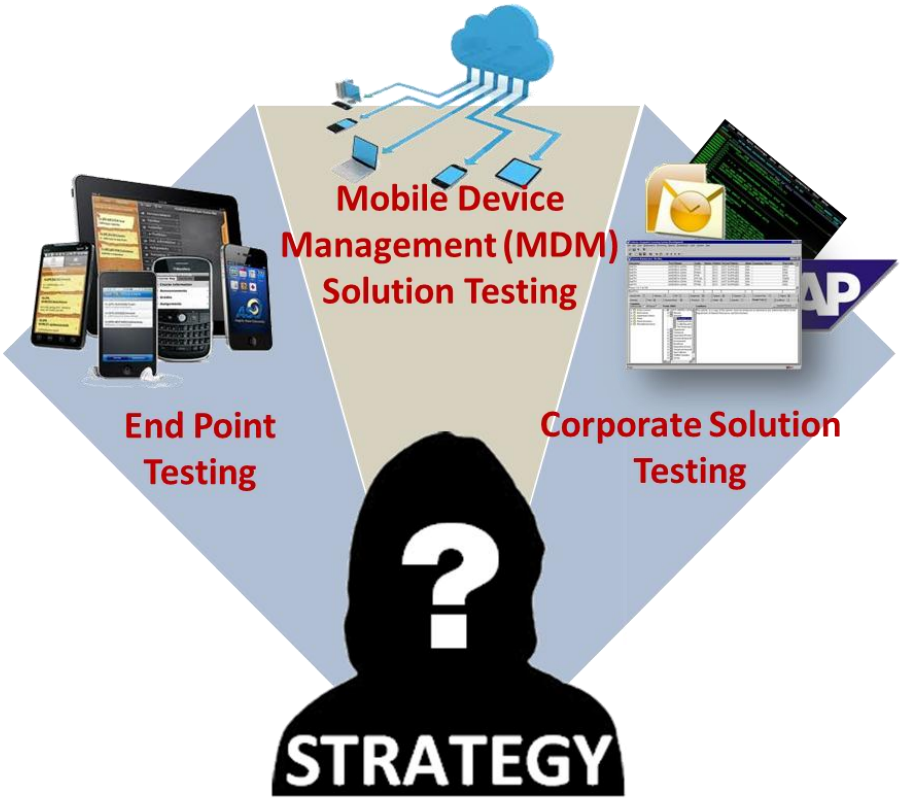
Developing an Effective Strategy

With all of the challenges facing organizations implementing BYOD the question become how to develop an effective testing strategy. Rather than simply focus on testing that employees have access to the desired applications, or testing that the devices remain secure, an effective strategy needs to take a Macro-to-Micro approach. So what is a Macro-to-Micro approach? This approach breaks down a testing in a top down strategy where the major components of the solution are identified, and a strategy for testing each component is devised. The component strategy identifies the sub components and specific strategies for that layer of the solution. This top down approach ensures an appropriate level of detail is understood for the components that make up the solution.

To make a simple example of the approach, let's think about how we would verify that a car was built correctly. We could take the approach of trying to brainstorm to figure out all of the features of the automobile that should be tested. For example, we could kick the tires, check the seats, check the oil, take a test drive, and so on. This approach would be a bottom up approach to identifying the strategy. If you think about it, the tester is just trying to think of all of the possible things that could be tested and hoping they cover everything. It is an approach that is down in the weeds, and likely to miss multiple issues. A better approach would be the top down approach where you break down the automobile into major components or systems. You have a body system; a power plant system, a drivetrain system; a comfort system; an interior system; a fuel system; and so on. The tester would select one of those systems, and then further break down that system into sub-components and sub systems. For example if we choose the power plant system, you could further break that system down into an exhaust system; a fuel delivery system; the coolant system; the piston & cylinder system; the head system; and so on. This approach ensures a much more detailed and systematic approach to testing, and will result in better defect removal.

The top down approach does not replace the need for end-to-end testing strategies that verify that all of the components of a system work together. An end-to-end testing strategy is critical to the success of any BYOD initiative. The challenge is that many organizations only focus on the end-to-end approach or simply focus on a single component of the overall system. In a BYOD implementation this may result in the primary focus being placed only on the MDM solution or the employee devices. An effective BYOD testing strategy focuses on the all aspects of the BYOD solution:

- End Point Testing
- MDM Solution Testing
- Corporate Solution Testing


Mobile Device Management (MDM) Solution Testing
End Point Testing
Corporate Solution Testing
AP
?
STRATEGY

Each major aspect of a BYOD implementation initiative needs to be considered when developing an effective test strategy. Teams may consider end point testing the devices that will be supported by the corporation, but what about the devices that are not going to be supported? How will you verify that they do not have access? Teams may consider testing the MDM solution and verifying that it can connect to the supported devices and deliver configurations, but what about the unique configuration of the MDM solution itself? How will you verify that the MDM has been configured correctly (e.g. workflow, policies, rules, etc.)? Teams may consider testing that the employee has access to the corporate solutions that are being enabled to employee devices, but what about the impact of the device on the corporate solution? Are you planning on verifying that the applications work correctly with the physical device and OS?

Effective Strategy Considerations

There are multiple testing considerations associated with each aspect of the BYOD implementation, End Point Testing, MDM Solution Testing, or Corporate Solution Testing. The sections that follow address a few of the testing considerations that should be made for BYOD testing. This is in no way an exhaustive list, and is intended only to stimulate your analytical juices and help kick start your strategy. The items to consider are in no particular order or priority. The order and priority of the items should be based on your organization's particular risk tolerance profile. If you are a small commercial software shop, you probably have a much higher tolerance for risk than a financial institution.

End Point Testing

End Point Testing. Probably the most obvious strategy area is end point testing. This testing focuses on the mobile device itself and whether or not the device is able to access the corporate applications, such as email, contacts, calendar, VPN, and so on, that the company has identified as part of the BYOD strategy. This testing may go so far as to ensure that the user is able to log into and effectively access any company applications. This type of testing can be characterized as "user experience" testing aimed at ensuring that the target applications are enabled and available for the end user.

In addition to "user experience" type testing, the testing organization should consider these additional strategies related to end point testing:

1) Test should be developed that ensure that all supported device, OS, carrier combinations function correctly. These tests should verify that the device is able to access the network, install the configurations from the MDM solution and correctly access the authorized corporate applications. Testing one version of iPad does not equal all versions of an iPad. Each iPad and OS combination has unique features and functions that they support. Because an application works on one combination does not project that it will work on all combinations. In a BYOD environment this poses a great challenge as the number of supported devices, OS and carrier combinations could be significant. For more on this read the *One More Thing* section at the end of this blog.

2) Tests should be considered that attempt to access the network using unsupported devices and OS versions. This strategy is designed to ensure that the system is proactively handling unsupported devices. There are multiple levels of consideration here. First, are users able to access the network with an unsupported device? Second, are they able to install the configurations from the MDM solution? And finally, are the users able to access the application from an unsupported device? Each of these tests addresses a separate portion of the end-to-end solution (e.g. Network, MDM, Corp App). A well-defined BYOD implementation will deny unsupported devices at every level of the solution.

3) Test the actual solutions that are installed on the mobile device. When an employee connects to the network for the first time, the MDM solution will install applications, such as virus protection on the employee device. For each device, OS, carrier combination make sure that the applications and services that are installed on the device work effectively and do not impact either the performance or the usability of the device. This will require that the testing group has the ability and tools to adequately assess security and performance on the device. Don’t forget to test that updates pushed out by the MDM are effectively handled by the device.

4) Test to ensure that all Personally Identifying Information (PII) is protected on the device. One of the legal considerations for corporations is access to and the protection of, employee’s PII. Your testing strategy should address how you will verify that the company doesn’t have access to personal data, including personal email, texts, photos, data, and more on the employee’s device. This should include testing to ensure that the company doesn’t have the ability to access the device’s location data, which may violate law in many jurisdictions.

5) There is a lot of testing that needs to be considered associated with testing the MDM solution installed on the device. This would include testing that the MDM policy enforcement functions correctly for events such as Jailbreaking or rooting attempts, as well as, the blocking of blacklisted applications. Testing should also be done to verify that data wiping works correctly when removing a device from the corporation without impacting the device owner's personal data (e.g. email, text, app data, photos, etc.).

Mobile Device Management (MDM) Solution Testing. The second are of testing strategy should be focused on the testing of the MDM solution itself. This testing should not only focus on verifying that the MDM solution as implemented in the organization’s infrastructure functions correctly. This testing focuses on the deployment of the application and functioning of the key features of the solution. While this implementation verification testing is important, it should not comprise the entire strategy for testing the MDM solution.

In addition to implementation type testing, the testing organization should consider these additional strategies related to MDM solution testing:

1) Tests should be developed that verify the “configuration” of the MDM solution. MDM solutions are purpose built to be highly configurable. As such, each organization must define the requirements and policies that will be configured in the MDM solution. The testing team needs to design testing strategies that verify that all configuration settings in the MDM solution are tested and function correctly.

2) Tests should also be defined that test the recurring features of the MDM solution, such as policy enforcement, data wiping, and update deployment. While most of the testing will be verified on the device side, the strategy needs to verify that the settings in MDM are effective. Testing may need to be developed to ensure that MDM management policies such as approvals and workflow function correctly.

3) Tests should be defined for any customization development that is done in association with the MDM implementation. This may be changes to network devices or policies, custom services, and so on. Implementing an MDM may require changes to legacy systems that support the enterprise. Caution should be taken to ensure that these changes are fully tested.

4) Just as in the case of end point testing, security and performance testing should be planned that focus on the MDM solution. With the monitoring of devices, and the deployment of updates to devices, there is the potential for the MDM solution to impact network performance. This should be verified through planned formal testing.

Corporate Solution Testing

Corporate Solution Testing. The final area for consideration in the testing strategy is the testing associated with the applications and services that are being delivered out to the mobile devices. Traditionally applications were deployed to networks, infrastructure, and end point solutions that were fully defined by and controlled by the organization. With the advent of BYOD, the absolute control of the end point has changed. No longer can organizations have confidence that their applications will be leveraged on a very limited set of devices, such as Blackberry. Now end users will access from iPhones, Androids, tablets, iPads, and more. This exponential explosion of supported devices posses a great risk to the corporate applications. While it the impact on enterprise level applications like email may be limited, the impact on internally developed solutions could have significant impact.

The testing organization should consider these additional strategies related to corporate solution testing:

1) Regression tests should be defined that verify that the corporate applications function fully on the supported devices. If the organization has traditionally only supported Blackberry devices they may have never tested the solution using a browser like Safari, Chrome, Mercury Web, Opera, Dolphin, etc. While browser is an easy example, the organization should focus on ensuring that all features and components of the application work adequately. This would include elements such as Flash, services, etc.

2) Tests should be defined that verify that corporate applications respond correctly to unsupported devices. As with the supported devices, the organization may have very narrowly tested the browsers that are supported. The application may need to be updated to reject unsupported browsers. I am often asked why this is important. I have had many a development manager tell me that we don't need to test against those other browsers because the corporate standards and corporate website clearly say they aren't supported. The challenge isn't the declaration; it is the unknown behavior of the application. If the unsupported browser doesn't correctly handle the application, there could be unintended consequences to the application behavior itself. The end user may actually receive behavior from the application that is detrimental to the user or the company. In either case, it is better to know what is going to happen or to prevent the possibility entirely by denying access to unsupported browsers.

3) Test strategies for all new applications and legacy systems have to be updated to now include the BYOD supported devices. This could result in a significant increase in the amount of testing effort to

conduct the testing of new features and regression testing. Organizations should consider the cost and impact of this testing as part of the overall impact and cost of going to a BYOD organizational strategy.

4) Performance & Security strategies need to be expanded to include the end-to-end security and performance of the application across multiple supported mobile devices, OS, and network combinations. This rapid expansion of supported systems can have a large impact on the performance of applications. If the company saves operational expenses on mobile devices, but rapidly loses the savings in loss of productivity due to poor performance and security issues, the BYOD initiative will be a failure.

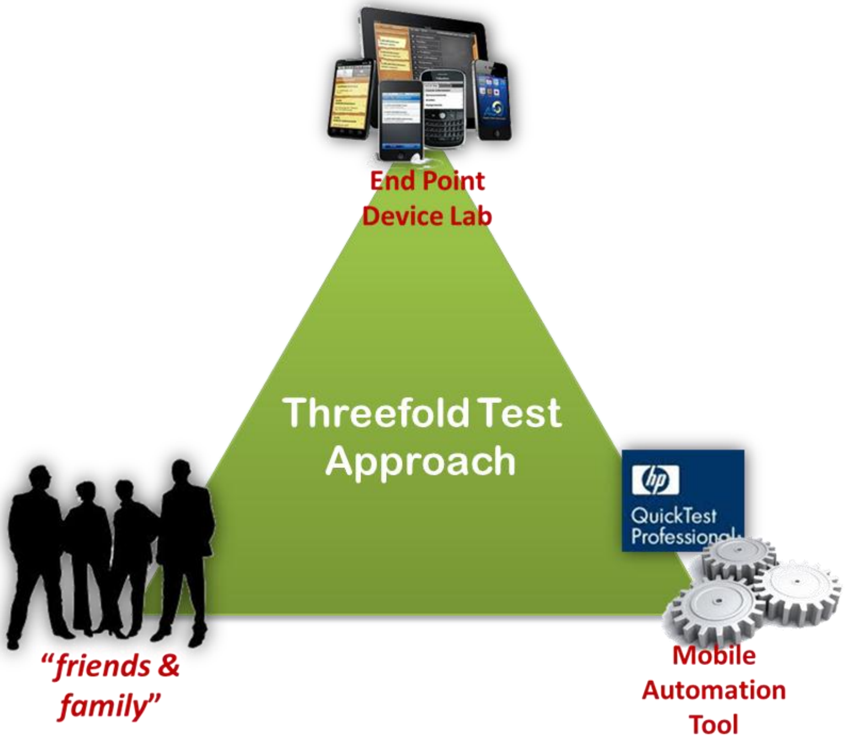
One More Thing: End Point Testing

Earlier I wrote about the significant challenge that faces many organizations as they consider testing on all supported device, OS, carrier combinations that are a part of the BYOD initiative. The number of devices that would be needed to support these combinations could easily be in the 100s. So the question becomes (1) how do you build out a mobile device Lab, or even if you can build a mobile device lab, and (2) is there even enough time to test all of these combinations even if you can build out a device lab.

We often hear from our clients that they are facing these tough questions. They struggle to even test a few devices; many times they use their personal devices to do the testing. While this temporarily solves the testing problem, it exposes the company to undue risk as these "test" devices are not controlled by or managed by the organization. The test team deploys the MDM on to the device; runs their test; and then hopefully removes the software and wipes the data from their device. Little or no automation is used to speed up the testing, which further reduces the ability of the team to fully test the solution.

I recommend a threefold approach to addressing as much of this problem as possible. First, I recommend that the enterprise collect statistics on the most frequently used device, OS, carrier combinations. This should be collected using automated network tools and surveys. From this list the organization can identify a critical subset of the devices to build out their lab. For the lab I recommend no less than two instances of each device. The reason for this is to ensure that you have a "0" and a "+1" device. The "0" device will match the current configuration of MDM and applications that are supported. The "+1" device is used to test new releases and updates.
The second part of the approach involves automation. A robust mobile automation solution should be implemented that integrates with your current automation solutions in use within your organization. For example, if your organization leverages the HP Unified Functional Test (UFT) solution, formerly known as QTP, make sure that the mobile solution integrates with UFT and allows you to use the core features of UFT, such as object recognition. Leveraging automation will allow you to test more devices faster, which will reduce risk.

The third and final approach I recommend is to implement a "*friends and family*" testing period. This is NOT a beta test or a pilot! This is a period where people who have previously been identified to have devices that you were not able to test are given access to the applications and are given specific testing tasks to accomplish. What makes this different is that the MDM solution should be delivered just as it is going to be delivered in production. It also means that these devices will need to be wiped by operations after testing is finished, and may require that the entire device get wiped (personal data and company data). The expectation is that multiple rounds of "*friends and family*" testing may need to occur based on defect discovery. This period should not be used as a "preview" to business leadership as there could be significant security and functional defects remaining in the BYOD environment.



Summary

Implementing a Bring Your Own Device strategy in an organization can be an excellent way to manage operational costs, but it is not without potential costs and risks. BYOD presents a challenge to the testing organization as the number of supported device combinations significantly increases the effort of testing. Creating an effective testing strategy involves ensuring that you have addressed the key components of the BYOD initiative.

- End Point Testing
- MDM Solution Testing
- Corporate Solution Testing

By considering test strategies that are specific to the components of a BYOD initiative you will significantly reduce the risk that your organization is exposed to. Addressing how you will test the solution and how you will build out your end point testing lab can significantly reduce the ongoing cost of supporting your enterprise. Happy testing.